Test result analysis of IPv6 Neighbor Discovery in a simple Wireless network
draft-sood-6man-nd-signalling-n-dad-test-00

Abstract

IPv6 WG is looking into various Neighbor Discovery (ND) optimization techniques. This document describes several test cases and test results on IPv6 ND number of messages, power usages using simple WiFi configuration and wireless phones as hosts.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document presents the test result analysis of several IPv6 ND test cases in a simple wireless network. Multiple test cases are performed on two different IPv6 ND implementations to show anomalies due to different power saving technique implementations on wireless devices.

IPv6 ND involves link-local discovery and address auto-configuration using multicast solicitation and advertisement messages. It provides a number of functionalities using link-local operations and, eases the configuration task for the administrator [SLAAC]. However, to increase the efficiency of the battery system, the power consumption due to the number of multicast messages exchanged in IPv6 ND process should be kept at minimum as per [I-D.vyncke-6man-mcast-not-efficient].

Several power saving techniques based on the sleep and wakeup interval of a device have been proposed. These techniques optimize the power by scheduling the node between cycles of sleep and wakeup [SOW]. It is the lack of any standardized technique that the devices from various manufacturers function differently and, pose challenges to automated management protocols like IPv6 ND [ND] and Stateless Address Auto-configuration (SLAAC) [SLAAC].

In this document, we present the test result analysis of different ND test cases using a simple wireless network.The difference in behavior comes from the implementation of the power saving techniques. We further show by analysis the difference in the number of ND messages exchanged between the devices due to different power saving techniques.

Section 2 describes the IPv6 SLAAC mechanism. Section 3 describes the current mechanism in sleep and wake up and the issues associated with it. Section 4 describes the experimental setup used. Section 5 describes the various test case scenarios and their expected behavior. Sections 6 presents the test case results regarding IPv6 ND implementation behavior and the number of multicast messages exchanged in different scenarios.

2. IPv6 Stateless Address Auto-configuration

In IPv6 SLAAC, the host generates a link-local address on system startup, and global addresses using the IPv6 prefix advertised by the routers on the same link. The host either listens to multicast router advertisement (RA) or sends multicast router solicitation (RS) messages. The link-local address and global IPv6 addresses remain

tentative unless they are verified to be unique by Duplicate Address Detection (DAD) algorithm. In DAD, a node checks the uniqueness of the IPv6 address by sending a neighbor solicitation (NS) message to the tentative IPv6 address as the destination address. The address gets assigned to an interface only if no other node responds to the NS message.

A general sequence of messages exchanged between the IPv6 host and the router is as shown below.

```
                    IPv6 Host                   IPv6 Router
                        +                            +
                        |                            |
                        |    Router Advertisement    |
           All Nodes    |<---------------------------+ Router Link
           MC Address   |                            | Local Address
                        |    Router Solicitation     |
           Node Link    +--------------------------->| All Routers
           Local Address|                            | MC Address
                        |    Router Advertisement    |
           All Nodes    |<---------------------------+ Router Link
           MC Address   |                            | Local Address
                        |  Multicast Listener Report |
           Node Link    +--------------------------->| All MLDv2-capable
           Local Address|                            | Routers
                        |             DAD            |
                        +--------------------------->|
           Unspecified  |                            | Solicited Node
           Address      |             DAD            | MC Address
                        +--------------------------->|
                        |                            |
                        |                            |
                        +                            +
```

Figure 1: Sequence of messages exchanged between IPv6 host and router

3. Sleep and Wakeup

The current increase in mobile services require efficient use of the battery power. The battery power usually lasts from few hours to few days. A number of power saving techniques are proposed to make the protocols energy efficient and thus increase the battery life [CO-PS] [CO-NODE]. These power saving techniques improve the energy consumption by optimizing the sleep and wake up pattern of the mobile host.

In this section, we present the current mechanisms in IPv6 for handling sleep and wake up and the issues related to it.

3.1. Current Mechanisms in Sleep and Wakeup

IPv6 ND [ND] does not provide any recommendations for handling sleep and wake up in mobile hosts. The general mechanism of the neighbor discovery and address auto-configuration require the destination host in the listening state. This idea of an "always on" host contrasts with the techniques used for power saving where the host has cycles of sleep and wake up time. During the sleep time, few power saving techniques keep the host listening to the incoming multicast messages while others completely shuts off all communication and goes to complete sleep.

[6LOWPAN-ND]suggest optimizations to ND by avoiding multicast messages except during system bootup or when the routers become unreachable.

3.2. Issues with the current mechanism

The non-standardization of the power saving techniques pose challenges to the current mechanisms in sleep and wake up for automatic IPv6 ND and SLAAC. These protocols function differently with power saving techniques which lead to serious security issues. Therefore [EFF-ND] suggest modifications to the legacy IPv6 ND for handling energy efficiency in a multicast network domain.

Issues in legacy IPv6 ND due to the power saving techniques depend on the below scenarios:

- o Sleep and wake up interval
- o Sleep and wake up pattern
- o Reachability to the routers on the same link
- o Address binding while in sleep mode and after wake up
- o Connectivity to other hosts while in sleep mode and after wake up

In the subsequent section, we present various experimental results to show the deficiencies of the current mechanism for handling sleep and wake up.

4. Experimental Setup

The experimental setup used is as shown in Figure 2. A Linux machine running Ubuntu 14.04 LTS is configured as an IPv6 router. IPv6 ND functionality is provided by the router advertisement daemon (radvd) in Linux router. Following are the minimal router configuration related to radvd and interfaces.

o radvd configuration

```
interface eth0
{
  AdvSendAdvert on;
  prefix 2001:db8:5::/64
  {
      AdvOnLink on;
      AdvAutonomous on;
  };
};
```

o Interface configuration

The eth0 interface on the IPv6 router is configured as below.

```
auto eth0
iface eth0 inet6 static
  address 2001:db8:5::1
  netmask 64
```

IPv6 forwarding is enabled in the sysctl.conf by setting net.ipv6.conf.all.forwarding to 1.

The router connects via its eth0 interface to the WAN port of the access point (AP). The configuration of the AP is manufacturer specific and should be done to allow IPv6 traffic to pass through it. The two IPv6 enabled wireless mobile stations (MS) namely MS A and MS B, connects to the AP via 802.11 wireless links; and the IPv6 Linux host connects to the AP via its Ethernet interface.

```
                  +------------+
                  |   Router   |
                  +------+-----+
                         |
                 +-------+------+
                 | Access Point |
                 +-------+------+
                         |
              +-------------------------+
              |          |              |
          +---+--+    +--+---+   +-----+-----+
          | MS A |    | MS B |   | Linux Host|
          +------+    +------+   +-----------+
```

Figure 2: Experimental Setup

5. Test Case Scenarios

The various test scenarios along with their expected behavior are discussed below:

Messages exchanged between the router and the MS on boot up:
When a MS boots up, it either solicits the router using multicast RS or listens to its multicast RA. The number of IPv6 addresses configured on the interface depends on the specific IPv6 implementations. The addresses are either global IPv6 privacy addresses, EUI-64 format addresses or both. The router also sends Multicast Listener Report messages to discover the presence of multicast listeners on the attached links [MLDv2].

Address binding when the MS is in sleep state:
The behavior of the MS in this scenario depends on the specific implementation of the power saving technique. MS either listens to the incoming messages in partial sleep state or shuts off all communication and goes to complete sleep.

Address binding when the MS wakes up:
When the MS wakes up, it checks for the uniqueness of the IPv6 address configured on its interfaces. The specific behavior in this scenario depends on the power saving technique used. If the MS continuously listens to the incoming multicast messages in partial sleep state, it still holds the interface IPv6 address. On the other hand, if the MS goes to complete sleep, it may or may not hold its configured IPv6 address.

Communication when the MS wakes up:
In this case, two scenarios are possible.

(1) Unique IPv6 address - An IPv6 host has unique IPv6 address in the network. Therefore, the host receives its intended communication.

(2) Duplicate IPv6 address - Two or more IPv6 hosts have same IP address in the network. Communication to these hosts depends upon the latest neighbor cache entries at the router. The host corresponding to the latest neighbor cache entry at router continues to receive the communication.

Number of multicast messages sent in the network
According to [ND], MinRtrAdvInterval is the minimum time allowed between sending unsolicited multicast RA from the interface, in seconds, and, MaxRtrAdvInterval is the maximum time allowed between sending unsolicited multicast RA from the interface, in seconds.

In this scenario, we have three different types of observation based on different values of MinRtrInterval, MaxRtrInterval, and AdvDefaultLifetime.

6. Test Case Results

In this section, we present the experimental results of different IPv6 ND implementation behavior. Next we present the detailed analysis of the number of multicast messages exchanged in different scenarios.

6.1. IPv6 ND Implementation Behavior

Based on the above test scenarios, below are the observations on the two IPv6 ND implementations.

Messages exchanged between the router and the MS on boot up:

(1) The number of messages exchanged between the router and the MS are tabulated below:

Type Of Message	MS A	MS B
Router Solicitation	1	1
Router Advertisement	1	1
Neighbor Solicitation	3	2
Neighbor Advertisement	0	0
Multicast Listener Report	4	2
Total Number of messages	9	6

Table 1: Number of multicast messages exchanged during boot up

(2) MS A on boot up generates two global IPv6 privacy addresses using the prefix advertised by the router. It also generates a link-local IPv6 address. MS A performs DAD for all the three IPv6 addresses.

(3) MS B on boot up generates two global addresses: an EUI-64 format address and the other as IPv6 privacy address using the prefix advertised by the router. It also generates a link-local address. It performs DAD only for the two global IPv6 addresses.

(4) The difference in the total number of messages is attributed to the difference in MLDv2 and NS messages. The number of MLDv2 messages exchanged depends upon the implementation. Also, MS B does not send NS message to check the uniqueness of the link local address.

Address binding when the MS is in sleep state:

(1) When MS A goes to sleep, any attempt to assign its global IPv6 address to the Linux host fails. This is because MS A keeps listening to the NS message from the Linux host during the DAD procedure and responds with NA message.

(2) When MS B goes to sleep, any attempt to assign its global IPv6 address to the Linux host succeeds. While asleep, MS B shuts off all communication. Any communication to MS B goes to the Linux host configured with MS B's global IPv6 address.

Address binding when the MS wakes up:

Both MS A and MS B does not perform DAD on wake up.

(1) MS A continuously listens to incoming messages while asleep, and thus do not need to perform DAD.

(2) MS B too does not check for the uniqueness of its IPv6 address via DAD in spite of coming out of complete sleep state.

Communication when the MS wakes up:

(1) MS A always keeps listening to incoming messages, so it's IPv6 address cannot be assigned to any other IPv6 host.

(2) In this scenario, the Linux host is assigned the IPv6 address of MS B which is in sleep state. All messages destined for MS B now goes to the Linux host. The Linux host continues to receive the messages until its entry lasts in the router neighbor cache. Once the router cache is flushed, either by manual intervention or by router boot up, the router solicits the solicited-node multicast address for link-layer address resolution. Linux host replies before MS B to this RA message. Since MS B entry is latest in the router cache, it again becomes the destination for all the messages.

6.2. Number of multicast messages

Below are the observations based on the number of multicast messages sent in the network.

Number of multicast RA messages sent in the network

The number of RA messages exchanged between the MS and the router for a duration of 5, 10, and 15 minutes are tabulated below:

Time Duration	Min/Max 30/70	Min/Max 30/150	Min/Max 30/300	Min/Max 30/600
5 minutes	8	4	4	3
10 minutes	15	6	5	3
15 minutes	18	13	8	4

Table 2: Number of RA messages exchanged

From the above table, we observe, as the difference between MinRtrAdvInterval and MaxRtrAdvInterval increases, the number of RA messages sent in the network reduces.

Total number of multicast messages sent in the network

The number of multicast messages exchanged between the MS and the router for a duration of 5, 10, and 15 minutes are tabulated below:

Time Duration	Min/Max 30/70	Min/Max 30/150	Min/Max 30/300	Min/Max 30/600
5 minutes	14	11	10	8
10 minutes	21	11	12	10
15 minutes	24	20	15	9

Table 3: Total number of multicast Messages exchanged

From the above table, we observe, as the difference between MinRtrAdvInterval and MaxRtrAdvInterval increases, the total number of messages sent in the network reduces.

Number of RA messages vs AdvDefaultLifetime

In this case, the number of RA messages exchanged between the MS and the router are observed with respect to AdvDefaultLifetime. AdvDefaultLifetime defines the lifetime of the router as a default router, and is measured in seconds.

The number of RA messages is measured with different values of AdvDefaultLifetime, MinRtrInterval and MaxRtrInterval for a duration of 5, 10, and 15 minutes and are tabulated below:

AdvDefaultLifetime	Min/Max	Number of RA
150	30/50	13
450	30/150	9
900	30/300	11
1800	30/600	9
2700	30/900	9
3600	30/1200	10
4500	30/1500	10
5400	30/1800	9

Table 4: Number of RA Messages vs AdvDefaultLifetime (5 minutes)

AdvDefaultLifetime	Min/Max	Number of RA
150	30/50	28
450	30/150	20
900	30/300	23
1800	30/600	21
2700	30/900	19
3600	30/1200	21
4500	30/1500	21
5400	30/1800	24

Table 5: Number of RA Messages vs AdvDefaultLifetime (10 minutes)

AdvDefaultLifetime	Min/Max	Number of RA
150	30/50	41
450	30/150	33
900	30/300	35
1800	30/600	29
2700	30/900	34
3600	30/1200	33
4500	30/1500	32
5400	30/1800	34

Table 6: Number of RA Messages vs AdvDefaultLifetime (15 minutes)

The frequency of messages depends upon the difference between MaxRtrAdvInterval and MinRtrAdvInterval. From the above tables, we observe, almost the same number of RA messages are sent by the router as for both high and low frequency cases. Only when the frequency is very high (for example MinRtrAdvInterval = 30 seconds and MaxRtrAdvInterval = 50 seconds), there is a surge in the number of RA messages.

7. Results Analysis

From the above test case analysis, we observe that considerable number of unsolicited RA messages are generated and those can be minimized. Also, in order to cope with battery power and IPv6 ND SLAAC behavior, implementations are coming up with independent solutions which can create serious security and reliability issues when the traffic of a sleeping host goes to another host configured with same IPv6 address. We also observe that the number of multicast messages are different in the two IPv6 ND implementations. These anomalies depends on vendors IPv6 implementation and the power saving techniques. In the next step, we target to test [EFF-ND] enhanced mode approach to observe the realiability and multicast message exchanges among multiple implementations.

8. Security Considerations

9. IANA Considerations

This memo includes no request to IANA.

10. Changelog

11. Acknowledgements

The author would like to thank Samita Chakrabarti for her valuable suggestions and insight on this work.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[EFF-ND] Chakrabarti, S., Nordmark, E., Thubert, P., and M. Wasserman, "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", draft-chakrabarti-nordmark-6man-efficient-nd-06 (work in progress), February 2014.

[6LOWPAN-ND] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "ND Optimizations for 6LoWPAN", RFC 6775, November 2012.

[ND] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6", RFC 4861, September 2007.

[SLAAC] Narten, T., Thomson, S., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[SOW] Tschofenig, H. and J. Arkko, "Report from the Smart Object Workshop", RFC 6574 , April 2012.

12.2. Informative References

[IPV6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6), Specification", RFC 2460, December 1998.

[I-D.vyncke-6man-mcast-not-efficient] Vyncke, E., Thubert, P., Levy-Abegnoli, E., and A. Yourtchenko, "Why Network-Layer Multicast is Not Always Efficient At Datalink Layer", draft-vyncke-6man-mcast-not-efficient-01 (work in progress), February 2014.

[CO-PS] Cao, Z., Gomez, C., Kovatsch, M., Tian, H., and X. He, "Energy Efficient Implementation of IETF Constrained Protocol Suite", draft-ietf-lwig-energy-efficient-01 (work in progress), October 2014.

[CO-NODE] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, May 2014.

[MLDv2] Vida, R. and L. Costa Eds, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

Author's Address

Ankur Sood
North Carolina State University
Raleigh, NC
USA

Email: asood2@ncsu.edu